CLAIMS

What is claimed is:

1   1.   A method for securely transferring data across an optical-switched (OS) network,

2   comprising:

3   distributing security keys to edge nodes in the OS network;

4   encrypting, at a source edge node, data to be sent from the source edge node to a

5   destination edge node, said data encrypted with a security key distributed to the source node;

6   sending the data along a virtual lightpath between the source and destination edge

7   nodes, the virtual lightpath spanning at least one lightpath segment; and

8   decrypting, at the destination edge node, the encrypted data that are sent.

1   2.   The method of claim 1, wherein the OS network comprises an optical burst-switched

2   (OBS) network.

1   3.   The method of claim 2, wherein the OBS network comprises a photonic burst-

2   switched (PBS) network.

1   4.   The method of claim 2, wherein the PBS network comprises a wavelength-division

2   multiplexed (WDM) PBS network.

1   5.   The method of claim 1, wherein the security keys are distributed by distributing a

2   common decryption and encryption key pair to each of the edge nodes.

1   6.   The method of claim 1, wherein the security keys are distributed by:

2   distributing a respective decryption key to each of the edge nodes, each respective

3   decryption key being particular to its node; and

4   distributing respective sets of encryption keys to each node, each set of encryption

5   keys for a given node including encryption keys corresponding to the decryption keys

6   distributed to each of the other edge nodes.

1   7.   The method of claim 1, wherein the security keys are distributed by:

2   distributing a respective private key to each of the edge nodes, each respective private

3   key being particular to its node; and

4   distributing respective sets of digital certificates sets to each node, each set of digital

5   certificates for a given node containing a set of public keys corresponding to the private keys

6   distributed to each of the other edge nodes.

1   8.   The method of claim 6, further comprising self-generating the digital certificates.

1   9.   The method of claim 8, further comprising:

2   for each edge node,

3   self-generating an digital certificate containing a public key that is asymmetric to the

4   private key for the edge node; and

5   sending the digital certificate to each of the other edge nodes.

1   10.   The method of claim 9, further comprising:

2   for at least one node,

3   generating a private key for the edge node via key-generation facilities provided by

4   the edge node; and

5   generating the public key for the edge node via the key-generation facilities.

1   11.   The method of claim 7, further comprising:

2   sending security data to a certificate authority, the security data defining public keys

3   that are to be included in respective digital certificates; and

4   receiving authenticated digital certificates from the certificate authority.

1   12.   The method of claim 11, wherein the security data is sent from an administrator of the

2   OBS network.

1   13.   The method of claim 9, further comprising:

2   generating a respective set of security data at each edge node; and

3   sending the respective set of security data from each edge node to the certificate

4   authority.

1   14.   The method of claim 1, further comprising sending security keys to the edge nodes

2   using a communication channel that is external to the OBS network to distribute the security

3   keys.

1   15.   The method of claim 1, further comprising sending security keys to the edge nodes

2   using an out-of-band channel of the OBS network to distribute the security keys.

1   16.   The method of claim 15, further comprising sending security data via a control burst

2   for the OBS network, the security data including one or more security keys or containing

3 . information from which one or more security keys can be derived.

1   17.   The method of claim 1, further comprising sending information to each edge node

2   identifying at least one of an encryption algorithm and decryption algorithm to be employed

3   to encrypt and/or decrypt the data via the security keys.

1 18.   The method of claim 17, further comprising sending encryption and/or decryption

2 code to an edge node, the encryption and/or decryption code to be executed to perform

3 encryption and/or decryption operations.

1 19.   A machine-readable medium to provide instructions, which when executed by a

2 processor in a source edge node of an optical switched (OS) network cause the source edge

3 node to perform operations including:

4   encrypting data to be sent to a destination edge node;

5   generating a control burst, the control burst containing information to reserve network

6 resources to form a virtual lightpath between the source edge node and the destination edge

7 node during a scheduled timeslot, the virtual lightpath including at least one lightpath

8 segment;

9   embedding information in the control burst identifying one or more data bursts to be

10 sent from the edge node to the destination edge node will be encrypted;

11   sending the control burst to a first hop along the virtual lightpath, the first hop

12 comprising one of a switching node or the destination edge node; and

13   sending said one or more data bursts containing the data that are encrypted to the first

14 hop along the virtual lightpath during the scheduled timeslot.

1 20.   The machine-readable medium of claim 19, wherein execution of the instructions

2 further perform the operation of sending an encryption key to each of a plurality of edge

3 nodes in the OS network.

1 21.   The machine-readable medium of claim 20, wherein execution of the instructions

2 performs the operation of sending the encryption key to an edge node by:

3   generating a control burst containing security data including the encryption key or

4   data from which the encryption key can be derived; and

5   sending the control burst to a first hop along a virtual lightpath coupling the edge

6   node sending the control burst to and edge node receiving the control burst, the first hop

7   comprising one of the edge node receiving the control burst or a switching node.

1   22.   The machine-readable medium of claim 21, wherein the security data include an

2   digital certificate.

1   23.   The machine-readable medium of claim 22, wherein execution of the instructions

2   performs the further operation of generating a self-signed digital certificate.

1   24.   The machine-readable medium of claim 21, wherein the security data include one of

2   information identifying an encryption algorithm used to encrypt the data or executable code

3   that may be used to decrypt the certificate.

1   25.   The machine-readable medium of claim 20, wherein an encryption key is sent to an

2   edge node via a communication channel that is external from the OS network.

1   26.   The machine-readable medium of claim 19, wherein execution of the instructions

2   performs further operations including:

3   generating an encryption key, the encryption key to be used to encrypt the data; and

4   generating a decryption key corresponding to the encryption key.

1   27.   The machine-readable medium of claim 19, wherein execution of the instructions

2   performs further operations including:

3   generating security data including the decryption key and identifying the decryption

4   key as a public key, the security data comprising data from which an digital certificate may

5   be issued; and

6   sending the security data to a certificate authority.

1   28.   A system comprising:

2   at least one processor;

3   memory coupled to said at least one processor;

4   an encryption component;

5   an optical interface; and

6   a storage device in which instructions are stored, said instructions to perform

7   operations when executed by said at least one processor, including:

8   invoking the encryption component to encrypt data to be sent to a destination

9   edge node operatively linked in communication to the system via a photonic burst-

10   switched (PBS) network, the system to operate as a source edge node;

11   generating a control burst, the control burst containing information to reserve

12   PBS network resources to form a virtual lightpath between the source edge node and

13   the destination edge node during a scheduled timeslot, the virtual lightpath including

14   at least one lightpath segment;

15   embedding information in the control burst identifying one or more data

16   bursts to be sent from the source edge node to the destination edge node will be

17   encrypted;

18   sending the control burst to a first hop along the virtual lightpath, the first hop

19   comprising one of a switching node or the destination edge node; and

20   sending said one or more data bursts containing the data that are encrypted to

21   the first hop along the virtual lightpath during the scheduled timeslot.

1 29.   The system of claim 28, wherein said at least one processor includes a network

2 processor.

1 30.   The system of claim 29, wherein said at least one processor includes an ingress

2 network processor and an egress network processor.

1 31.   The system of claim 30, wherein the encryption component comprises a hardware

2 device programmed to perform encryption operations.

1 32.   The system of claim 30, wherein the encryption component is embodied as a software

2 module comprising a plurality of instructions to effectuate encryption operations when

3 executed on a processor.

1 33.   The system of claim 28, further comprising a decryption component configured to

2 decrypt data received from the PBS network.

1 34.   The system of claim 33, wherein the decryption component comprises a hardware

2 device programmed to perform decryption operations.

1 35.   The system of claim 33, wherein the decryption component is embodied as a software

2 module comprising a plurality of instructions to effectuate decryption operations when

3 executed on a processor.

1 36.   The system of claim 28, further comprising a key generation component.

1 37.   The system of claim 36, wherein the key generation component comprises a hardware

2 device programmed to generate security keys.

1   38.   The system of claim 36, wherein the key generation component is embodied as a

2   software module comprising a plurality of instructions to effectuate generation of security

3   keys.